REPLY TO
ATTENTION OF:

CEMP-OC

0 8 MAY 2007

MEMORANDUM FOR Commanders, Directors, and Chiefs of Separate Offices

SUBJECT: Operations Security (OPSEC) Policy Letter

1. Operations Security is a vital component of every operation civil and military. Headquarters USACE and each Major Subordinate Command will establish an Operations Security Working Group.

2. Operations Security is an analytic process used to deny an adversary information. OPSEC analysis is used to: identify those actions that can be observed by adversary intelligence systems; determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

3. Identifying and protecting observable critical information of military plans, operations, and supporting activities from adversary observation and collection is, therefore, the primary goal of OPSEC. Operations Security measures are then developed to eliminate, reduce, or conceal the indicators that can reveal critical information. Critical Information can be either classified or unclassified and is information that is so crucial to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it, the compromise of this information could prevent or seriously degrade mission success.

4. Operations Security needs to be enacted in all aspects of your day-to-day activities: on the phone, in your e-mails, and in conversations where those without a "need-to-know" might overhear. Operations Security supplements traditional security measures for protecting potentially exploitable information.

5. The point of contact is the Headquarters Operations Security Manager, John Brown, at John.F.Brown@usace.army.mil.

CARL A. STROCK
Lieutenant General, US Army
Commanding